

# APPENDIX

## I

METHOD, COMPUTER PROGRAM, AND CONTROL DEVICE FOR  
OPERATING A VEHICLE IN A RESTRICTED MODE OF  
OPERATION

BACKGROUND AND SUMMARY OF THE INVENTION

[0001] This invention relates to a method, a computer program and a control device for operating a vehicle in a mode of operation which can be activated by its user and which is restricted compared with a normal mode of operation of the vehicle.

[0002] In situations in which the vehicle must be left to a third person, for example if the vehicle has to be handed to a workshop for repair purposes or to the porter of a hotel for parking, it is desirable, in particular, if the vehicle could be handed over with a mode of operation which is only restricted compared with a normal mode of operation. Ideally, the restricted mode of operation should allow operation of the vehicle by the third person only as much as is required in the individual case. The restricted mode of operation would then provide protection of the vehicle against misuse and theft by the third person.

[0003] Prior art methods, computer programs and control devices are known which allow the user of a vehicle to place the vehicle into a restricted mode operation. In German document DE 199 61 619 A1, for

example, it is disclosed that the use of a vehicle by certain persons can be restricted to certain times and these times, can be individually specified as part of a personalization function.

[0004] Furthermore, limiters and cruise controllers are known in the prior art. Both devices make it possible to restrict the mode of operation of the vehicle in as much as its maximum speed can be limited. In the case of a limiter, the restricted speed is permanently set.

[0005] In the case of a cruise controller, by comparison, the restricted operating mode, i.e. the predetermined maximum speed, can be varied by the user at any time, and completely cancelled again by accelerating. Moreover, it is automatically deactivated by switching off the ignition of the vehicle. Such known control devices, as they are currently constructed, are, therefore, not suitable as protection for a vehicle against misuse and theft.

[0006] On the basis of this prior art, it is the object of the invention, therefore, to develop a known method, computer program and control device for operating a vehicle in a restricted mode of operation in such a manner that the vehicle is protected against theft and/or misuse by the restricted mode of operation.

[0007] This object is accordingly achieved by the fact that the restricted mode of operation can only be deactivated again by an authorized person who does not need to be identical to the user.

[0008] “User” in the sense of the invention is any person who, authorized or unauthorized, has power of disposal over the vehicle and can drive it. In the normal case, this is the owner or the current driver of the vehicle but it can also be a third person to whom the vehicle has been left by the owner for his use, or a third person who is using the vehicle illegally.

[0009] In distinction from the user defined in this manner, the term “authorized person” in the sense of the invention only means a much more restricted circle of persons. In particular, this term includes the owner of the vehicle and persons expressly authorized by him for deactivating the restricted mode of operation. As a rule, persons to whom the vehicle has been left only for a limited time or, respectively, for a particular purpose, and persons who are illegally using the vehicle, are not included in the circle of authorized persons, in distinction from the circle of users.

[0010] Due to the claimed restriction that the restricted mode of operation can only be deactivated by an authorized person, it is ensured, according to the invention, that the full range of functions is

not available to the respective user of the vehicle which is why misuse or theft of the vehicle would either not be possible at all or senseless.

[0011] In a first advantageous exemplary embodiment of the method, the restricted mode of operation is automatically restored even after the ignition has been switched off and the vehicle subsequently restarted, as long as it has not been deactivated again by the authorized person. This is therefore of importance, especially for the reason that the theft protection implemented by the restricted mode of operation cannot be eliminated or bypassed, respectively, by simply switching off the vehicle.

[0012] Whereas the restricted mode of operation can be advantageously activated without checking the user, authentication of this authorized person is absolutely mandatory before the restricted operating mode can be deactivated by the authorized person. It is only the authentication which ensures that the person who is currently attempting to deactivate the restricted mode of operation is actually authorized to do this. The two physically separate processes of authentication and deactivation can be implemented in such a manner that they are triggered by the user by performing either only one operating step or two separate operating steps individually allocated to the two processes.

[0013] The restriction of the operating mode of the vehicle can be advantageously implemented in a different manner. On the one hand, it can consist of a restriction of the driving mode of the vehicle; on the other hand, the restriction can be a restriction of the utilization of the vehicle by the user and/or a restriction in the access rights of the user of the vehicle to person-related data which are accessible via devices associated with the vehicle.

[0014] It is also of advantage if the range of restriction in the restricted mode of operation can be redefined again at any time, preferably under menu control or by voice input.

[0015] The abovementioned object of the invention is also achieved by a computer program with program code for carrying out the method described above, a data medium with a corresponding computer program, and by a control device for operating a vehicle in a restricted mode of operation. The advantages of these further solutions of the object correspond to the advantages mentioned above with respect to the claimed method.

[0016] Further advantageous embodiments of the method, of the computer program, and of the control device are the subject matter of the dependent claims.

## BRIEF DESCRIPTION OF THE DRAWINGS

[0017] Figure 1 shows a control device according to the invention;

[0018] Figure 2 shows an example of the implementation of the restricted mode of operation; and

[0019] Figure 3 shows a further example for implementing the mode of operation restricted according to the invention.

## DETAILED DESCRIPTION OF THE INVENTION

[0020] In the text which follows, the invention will be described in detail in the form of numerous exemplary embodiments and with reference to said figures.

[0021] Figure 1 shows the control device 100 according to the invention. The control device 100 is used for operating a vehicle (not shown) in a mode of operation which is restricted compared with a normal mode of operation as is usually available when the vehicle is supplied by the manufacturer. For adjusting and operating this restricted mode of operation, the control device 100 comprises a memory device 110 in which the range of the restricted mode of operation is stored/defined. In addition, an input device 120 is associated with the control device 100 for activating the restricted mode of operation by the

user of the vehicle. The input device 120 is preferably constructed in a form of a keyboard with or without an additional screen so that it provides for a manual, preferably menu-controlled, input. As an alternative or in addition to a manual input, a voice-controlled input can also be provided.

[0022] Whatever the construction of the input device 120, activation A of the restricted mode of operation acts directly on a control device 140. Due to the activation, the control device 140 is instructed to load a restricted mode of operation, selected by a respective input, out of the memory device 110 and to implement said mode of operation by driving components 150-1...-N of the vehicle. The components will be explained in greater detail below in conjunction with the possible range of the restricted mode of operation.

[0023] Advantageously, however, the input device 120 is used for not only activating a predetermined mode of operation, but instead also for the individual modification M thereof. For this purpose, it is connected directly to the memory device 110. The modification M enables the restricted mode of operation to be individually adapted to a respective situation. It may thus be appropriate that in the case where the vehicle has to be left at a workshop for repair purposes, a different restricted mode of operation is suitable than if the vehicle is left to the porter of a hotel for parking.



[0024] So that the restricted mode of operation in the sense of the invention can be used for protecting the vehicle against misuse or theft, an authentication device 130 is provided according to the invention which is connected between the input device 120 and the control device 140. The authentication device 130 ensures that deactivation D of the restricted mode of operation in the vehicle can only be effected by a person authorized therefor. To check the person with regard to his/her authorization, the input device 120 and the authentication device 130 can be constructed differently in each case. If, for example, the input device 120 is constructed for reading-in biometric features in the form of a fingerprint of a person, the subsequent authentication device 130 should be constructed for comparing the fingerprint read in with the fingerprint of the authorized person with regard to a match. As an alternative or additionally, the input device 120 can be constructed for reading-in a personal identification number (PIN); in this case, the authentication device 130 should also be alternatively or additionally constructed for comparing the PIN read in with a PIN allocated to the authorized person, with regard to a match. In both cases it holds true that the authentication device 130 forwards the command for deactivation D of the set mode of operation, delivered by the respective person via the input device 120, to the control device 140 only if at least one of the two comparisons results in a match.

[0025] Also alternatively or as a supplement to the above possibilities, the authentication device 130 can also be constructed to effect the authorization of a person in interaction with a service center located, as a rule, remotely, for example an emergency service. For this purpose, the authentication device 130 has a communication device 132 in order to obtain information about the authorization or nonauthorization of a person from the service center, preferably by radio link. Such a procedure can be considered, in particular, when a person who wishes to perform a deactivation D has forgotten his/her PIN, for example, but can prove himself/herself to be authorized to the service center.

[0026] According to the invention, there are basically three possibilities for the type of restriction in the restricted mode of operation, and these three possibilities can be implemented not only singularly but also in combination with one another.

[0027] A first possibility consists in a restriction of the driving mode of the vehicle by a manipulation of its vehicle-related data F. During this process, for example, a maximum speed which is below the speed which is made possible by the manufacturer and/or a maximum distance which can be traveled by the vehicle during the activation of the restricted mode of operation, can be preset. In the case where the vehicle is left to the porter of a hotel for parking, for example, it may be

sufficient to limit the maximum speed of the vehicle to 40 km/h (24.8 mph) and the maximum traveling distance of the vehicle to, for example, 100 m (328 ft). This makes it possible to ensure that the porter will not misuse the vehicle for a spin around town or even steal the vehicle. Implementation of this restriction of the driving mode requires that the control device evaluates, for example, the speed signal of the vehicle, position pick-up signals or global positioning system GPS signals with respect to the preset limitations and, if necessary, acts appropriately on the brakes, the steering or the power supply etc. as components 150-1...-N of the vehicle. When the predetermined maximum speed has been reached, this action can, for example, be that further stepping on the gas pedal is prevented, or that after the predetermined maximum distance has been reached, releasing the brakes or reactivating the power supply is impossible.

[0028] A second possibility for restriction is that the user is prevented from using certain parts or areas of the vehicle. Thus, for example, access to the glove box or the trunk of the vehicle can be denied to him/her. For this purpose, suitable locking devices must be provided at the respective devices such as glove box or trunk as components 150 which, when necessary, are driven in a suitable manner by the control device 140.

[0029] As a third possibility, a restriction in the access rights of the user to person-related data can be provided, which data are basically accessible through devices in the vehicle such as, for example, a PC or a navigation system. In the case of these person-related data, a distinction is preferably made between non-sensitive and sensitive data, that is to say particularly sensitive data. Examples of the non-sensitive person-related data are adjustments of seats or the adjustments of volume of the radio which can be stored individually in the sense of a personalization concept for individual persons who occasionally utilize the vehicle. By comparison, the sensitive person-related data are, for example, e-mails which have been received or sent by a certain person or navigation data, for example destinations which the person has driven to in the past or wishes to drive to in the future. A restriction with respect to these person-related data is preferably implemented by the fact that only a write protection is set up for the non-sensitive data but both a read-protection and a write protection are set up for the restricted mode of operation for the sensitive data.

[0030] Figure 2 illustrates the case where person-related data of only one person P1 are stored in the vehicle. Advantageously, the non-sensitive data NSDP1 stored for this person can then be stored, for example, for initialization purposes, in the memory device 110 as part of the restricted mode of operation. It is important that an initialization is specified for certain devices such as seats or hi-fi systems also in the

case of a restricted mode of operation so that the driving devices for these systems know how they should respond or, respectively, what adjustments they should perform. In the example shown, the non-sensitive person-related data NSDP1, which have already been stored in any case, simply only need to be copied into the memory device 110; initialization of the corresponding devices is then possible by a simple read access of these data.

[0031] In contrast to the non-sensitive data NSDP1, the sensitive data SDP1 are not required for initializing devices, as a rule. Naturally, a personal computer PC or a navigation device in the vehicle must also be initialized in the restricted mode of operation, but this initialization is usually automatic when the ignition is switched on. The contents of individual e-mails, however, are not used for initializing the PC any more than individual navigation destinations are required for initializing the navigation system. These data SDP1 should, therefore, remain unnoticed in the definition of the restricted mode of operation and not be transferred into the memory device 110.

[0032] Figure 3 shows a case similar to Figure 2, the difference being that person-related data of not only one but three persons P1, P2, P3 are stored in the vehicle. More precisely, sensitive data SDP1, SDP2, SDP3 and non-sensitive data NSDP1, NSDP2, NSDP3 are then in each case known of these three persons. In this case, too, it is appropriate to

access the sensitive data of only one person, for example of person P1, for initialization purposes when setting the restricted mode of operation. The non-sensitive data of the other persons P2 and P3 and the sensitive data SDP1...3 should preferably not be transferred into the memory device 110 and used for defining the restricted mode of operation.

[0033] In contrast to the person-related data, it is generally not possible to use a particular data record which is stored somewhere in the vehicle, in any case, with respect to the vehicle data F. As a rule, they must be defined individually for each restricted mode of operation, preferably via the input device 120 as mentioned above.

[0034] For the deactivation D of the restricted mode of operation by the authorized person, various variants are also conceivable with respect to the person-related data. A first variant consists in that, in this case, the person-related data of all persons affected P1...3 are released again for reading and/or writing. As an alternative, it is conceivable that in this case only the person-related data of only individual persons, particularly of the authorized person him/herself, are released again for reading and/or writing. Advantageously, the sensitive person-related data, in particular, are protected by individual passwords.

[0035] The method described above for defining, activating and deactivating the restricted mode of operation in a vehicle is advantageously implemented in the form of a computer program. Such a computer program can be stored, for example, possibly together with other computer programs, on a computer-readable data medium. The data medium can be a floppy disk, a compact disk, a flash memory or the like. The computer program stored on the data medium can then be sold to a customer as a product.

[0036] In the case of implementation as computer program, it is also possible that the computer program, possibly together with other computer programs, is transferred to a customer as product for the control device according to the invention via an electronic communication network, particularly the Internet – without the aid of a data medium - and is sold in this manner.